HKUST – Department of Computer Science and Engineering
COMP 2711: Discrete Math Tools for CS – Fall 2014

Serial #

Final Examination

Date: Tuesday, 16 December 2014 Time: 4:30pm–7:30om

Name: _____	Student ID: _____
Email: _____	Lecture and Tutorial: _____
Program (circle one): COMP BBA+COMP others	

Instructions

- This is a closed book exam. It consists of 17 pages and 10 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap papers and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Some questions can be answered using only a few lines.
- **Unless otherwise specified you *must* always explain how you derived your answer. A number without an explanation will be considered an incorrect answer.**

Questions	1	2	3	4	5	6	7	8	9	10	Total
Score											

Student ID: _____

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Student ID: _____

Problem 1: [10 pts] Consider a game of throwing two fair dice. You lose one dollar if the two dice have different number of dots on top. You win d dollars if both dice have d dots on top. Let X denotes the amount of dollars you win.

(a) What is the expected value of X if you play this game once?

(b) What is the variance if you play this game once?

(c) What is the expected value of X if you play this game n times?

(d) What is the variance of X if you play this game n times?

Explain how your answers are derived.

Answer: (a) The probability that you lose in the game is $5/6$, you win 1 dollar in the game is $1/36$ as well as you win $2, 3, 4, 5$ and 6 dollar. Thus $E(X) = (-1)(5/6) + 1/36 + 2/36 + 3/36 + 4/36 + 5/36 + 6/36 = (21 - 30)/36 = -1/4$

(b) $V(X) = 5(-1+1/4)^2/6+(1+1/4)^2/36+(2+1/4)^2/36+(3+1/4)^2/36+(4+1/4)^2/36+(5+1/4)^2/36+(6+1/4)^2/36 = 475/144$

(c) By the linearity of expectation, the expected value is $-n/4$.

(d) The n trials are independent, thus the variance is $475n/144$

Student ID: _____

Problem 2: [10 pts]
Let a, m and n be three positive integers that are larger than 1. Is each of the following statements true or false? If it is true, give a proof. If it is false, give a counterexample.

(a) $(a \bmod mn) \bmod n = a \bmod n$.

(b) $(a \bmod mn) \bmod n = a \bmod m$.

(c) If $a \bmod n = 1$, then $gcd(a, n) = 1$.

(d) If $gcd(a, n) = 1$, then $a \bmod n = 1$.

Answer: (a) This is true. According to Euclid's Division Theorem, there exist q_1 and r_1 such that

$$a = q_1 mn + r_1, \qquad 0 \le r_1 < mn,$$

where $r_1 = (a \bmod mn)$. Similarly, there exist q_2 and r_2 such that

$$r_1 = q_2 n + r_2, \qquad 0 \le r_2 < n,$$

where $r_2 = r_1 \bmod n = (a \bmod mn) \bmod n$. Combining the two equations, we get

$$a = (q_1 m + q_2)n + r_2, \qquad 0 \le r_2 < n.$$

Hence, $a \bmod n = r_2$. Consequently,

$$(a \bmod mn) \bmod n = r_2 = a \bmod n.$$

(b) This is false. Let $a = 8$, $m = 2$ and $n = 3$. We have

$$(a \bmod mn) \bmod n = (8 \bmod 6) \bmod 3 = 2,$$
$$a \bmod m = 8 \bmod 2 = 0.$$

(c) This is true. $a \bmod n = 1$ implies that there exist q such that $a = qn + 1$, or $a - qn = 1$. The latter equation implies that any common divisor of a and n must divide 1, hence must be 1. Therefore, $gcd(a, n) = 1$.

(d) This is false. For example, $gcd(5, 3) = 1$, but $5 \bmod 3 = 2$.

Student ID: _____

Problem 3: [12 pts]
Consider the following simplified version of the RSA algorithm for public cryptography:

(i) Bob's public key is a pair (n, e), where n is a prime number and e is a positive integer that is smaller than n and is relatively prime with $n - 1$.

(ii) Bob's private key is $d = e^{-1} \bmod (n - 1)$.

(iii) Alice encrypts a message m $(0 < m < n - 1)$ by calculating $c = m^e \bmod n$, and sends the ciphertext c to Bob.

(iv) Bob decrypts the ciphertext c by calculating $c^d \bmod n$.

Suppose $n = 251$ and $e = 137$.

(a) Calculate d using the extended GCD algorithm. Show the computational steps.

(b) Suppose $m = 200$. Calculate $c = m^e \bmod n$ using repeated squaring. Show the computational steps.

(c) Is the system secure? Explain why or why not.

[MORE SPACE ON NEXT PAGE]

Answer: (a) Repeatedly using Euclid's Division Theorem, we get

$$\begin{aligned} 250 &= 1 \cdot 137 + 113 \\ 137 &= 1 \cdot 113 + 24 \\ 113 &= 4 \cdot 24 + 17 \\ 24 &= 1 \cdot 17 + 7 \\ 17 &= 2 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \end{aligned}$$

Rolling back, we get

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17 \\ &= 5 \cdot (24 - 17) - 2 \cdot 17 = 5 \cdot 24 - 7 \cdot 17 \\ &= 5 \cdot 24 - 7 \cdot (113 - 4 \cdot 24) = 33 \cdot 24 - 7 \cdot 113 \\ &= 33 \cdot (137 - 113) - 7 \cdot 113 = 33 \cdot 137 - 40 \cdot 113 \\ &= 33 \cdot 137 - 40 \cdot (250 - 137) = 73 \cdot 137 - 40 \cdot 250. \end{aligned}$$

Therefore, $d = 73$.

[WORK SPACE FOR PROBLEM 3]

(b) Observe that $137 = 2^7 + 2^3 + 2^0$. Using repeated squaring, we get

$$\begin{aligned} I_0 &= 200 \\ I_1 &= 200 \cdot 200 \bmod 251 = 91 \\ I_2 &= 91 \cdot 91 \bmod 251 = 249 \\ I_3 &= 249 \cdot 249 \bmod 251 = 4 \\ I_4 &= 4 \cdot 4 \bmod 251 = 16 \\ I_5 &= 16 \cdot 16 \bmod 251 = 5 \\ I_6 &= 5 \cdot 5 \bmod 251 = 25 \\ I_7 &= 25 \cdot 25 \bmod 251 = 123 \end{aligned}$$

So,

$$c = I_7 \cdot I_3 \cdot I_0 \bmod 251 = 123 \cdot 4 \cdot 200 \bmod 251 = 8.$$

(c) The system is not secure because the adversary can easily compute the private key d from the public key (n, e).

Student ID: _____

Problem 4: [10 pts]
In this question we consider the following modular equations:

$$\begin{aligned} x \bmod m &= a \\ x \bmod n &= b \end{aligned}$$

For each of the following parts, does there exist an integer x, $0 \leq x < mn$ that satisfies the two equations?

(a) $m = 15$, $n = 16$, $a = 5$, $b = 2$.

(b) $m = 30$, $n = 16$, $a = 5$, $b = 2$.

If yes, find the solution and show the computational steps. Otherwise, prove by contradiction that there does not exist a solution.

In this question, it is up to you whether to use the extended GCD algorithm to find multiplicative inverses. If you choose to use it, there is no need to show the steps.

[MORE SPACE ON NEXT PAGE]

Answer: (a) In this case, m and n are relatively prime. So,there is a solution. To find the solution, first compute multiplicative inverses:

$$\bar{m} \quad s.t. \quad m \cdot \bar{m} = 1 \bmod n,$$

$$\bar{n} \quad s.t. \quad n \cdot \bar{n} = 1 \bmod m.$$

It turns out that $\bar{m} = 15$ and $\bar{n} = 1$. Now we can find the solution:

$$\begin{aligned} x &= (an\bar{n} + bm\bar{m}) \bmod mn \\ &= (5 \cdot 16 \cdot 1 + 2 \cdot 15 \cdot 15) \bmod 15 \cdot 16 \\ &= 50 \end{aligned}$$

(b) Assume there is a solution x. Then there exist integers q_1 and q_2 such that

$$\begin{aligned} x &= q_1 \cdot 30 + 5, \\ x &= q_2 \cdot 16 + 2. \end{aligned}$$

Hence we have

$$q_2 \cdot 16 - q_1 \cdot 30 = 5 - 2 = 3.$$

This equation cannot be satisfied because the left hand side is divisible by 2, while the right hand side is not. Therefore, there is no solution.

Student ID: _____

[WORK SPACE FOR PROBLEM 4]

Student ID: _____

Problem 5: [10 pts] For each of the following pairs of logic statements, either prove that the two statements are logically equivalent, or give a counterexample. In your proof, you may use either a truth table or logic laws. A counterexample should consist of a truth setting of the variables and the truth values of the statements under the setting.

(a) $(p \wedge \neg q) \Rightarrow (r \wedge \neg r)$ and $p \Rightarrow q$

(b) $\exists x \in U\ p(x) \Rightarrow \exists x \in U\ q(x)$ and $\exists x \in U(p(x) \Rightarrow q(x))$

(c) $\exists x \in U\ p(x) \Rightarrow \forall y \in V\ q(y)$ and $\forall x \in U\ \forall y \in V(p(x) \Rightarrow q(y))$

Answer: (a) Equivalent.

$$\begin{aligned}(p \wedge \neg q) \Rightarrow (r \wedge \neg r) &\equiv \neg(p \wedge \neg q) \vee (r \wedge \neg r)\\ &\equiv \neg p \vee q \vee F\\ &\equiv \neg p \vee q\\ &\equiv p \Rightarrow q\end{aligned}$$

(b) Not equivalent. Counterexample:

- U: All animals; $p(x)$: x can fly; $q(x)$: x can fly airplane.
- LHS is false because there are animals that can fly, but no animal can fly airplane.
- RHS is true because there are animals that cannot fly and hence $p(x) \Rightarrow q(x)$ is true.

(c) Equivalent.

$$\begin{aligned}\exists x \in U p(x) \Rightarrow \forall y \in V q(y) &\equiv \neg(\exists x \in U p(x)) \vee (\forall y \in V q(y))\\ &\equiv (\forall x \in U \neg p(x)) \vee (\forall y \in V q(y))\\ &\equiv \forall x \in U \forall y \in V(\neg p(x) \vee q(y))\\ &\equiv \forall x \in U \forall y \in V(p(x) \Rightarrow q(y))\end{aligned}$$

Student ID: _____

Problem 6: [10 pts]
Prove the following statements. You may use a direct proof, a proof by contraposition or a proof by contradiction as appropriate.

(a) $\sqrt{3}$ is an irrational number.

(b) If m and n are integers such that mn is even, then m is even or n is even.

Answer: (a) Suppose $\sqrt{3}$ is rational. Then there are integers m and n with no common factors so that $\sqrt{3} = m/n$. Squaring both sides gives $3 = \frac{m^2}{n^2}$, or $m^2 = 3n^2$. This implies that 3 divides m^2. Together with the fact that 3 is prime, we have 3 divides m. Let $m = 3k$ for some integer k. Substituting into $3n^2 = m^2$, we have $3n^2 = (3k)^2$, thus $n^2 = 3k^2$, which implies 3 divides n^2. Therefore, 3 divides n. Hence both m and n have a common factor of 3. But this contradicts the supposition that m and n have no common factors.

Another way to argue for contradiction: m^2 has even number of factors in its prime factorization, while $3n^2$ has odd number of factors.Therefore, they cannot be equal.

(b) Suppose m and n are both odd. $m = 2k + 1$ for some integer k and $n = 2h + 1$ for some integer h. Then $mn = (2k + 1)(2h + 1) = 2(2kh + k + h) + 1$, which is odd.

Student ID: _____

Problem 7 : [8 pts] Let n be a positive integer. Use induction to prove that, for any non-negative integer m, there exist integers q and r such that

$$m = qn + r, \quad 0 \leq r < n. \tag{1}$$

- **Proof by weak induction:**
  Base Case: If $m < n$, we set $q = 0$ and $r = m$. Then (1) is true.
  Induction Hypothesis: Assume (1) is true for the case of $m - 1$. That is, there exist q' and r' such that

$$m - 1 = q'n + r', \quad 0 \leq r' < n.$$

  Inductive Step: Now consider the case of m. There are two cases:

  (a) $r' < n - 1$. In the case, we set $q = q'$ and $r = r' + 1$. Then (1) is true.

  (b) $r' = n - 1$. In the case, we set $q = q' + 1$ and $r = 0$. Then (1) is true.

  By the principle of Mathematical Induction, we conclude that (1) is true for all non-negative integers m.

- **Proof by strong induction**:

  Base Case: If $m < n$, we set $q = 0$ and $r = m$. Then (1) is true.
  Induction Hypothesis: Assume (1) is true for any non-negative integer w such that $n \leq w < m$.
  Inductive Step: Now consider the case of $n \leq m$. Let $w = m - n$. By the induction hypothesis, there exist q' and r' such that

$$w = q'n + r', \quad 0 \leq r' < n.$$

  Hence,

$$m = w + n = (q' + 1)n + r'.$$

  So, if we set $q = q' + 1$ and $r = r'$, then (1) is true.

  By the principle of Mathematical Induction, we conclude that (1) is true for all non-negative integers m.

Student ID: _____

Problem 8: [10 pts]
Let a be a real number such that $a > 1$. Consider a function $T(n)$ over integers defined as follows

$$\begin{aligned} T(0) &= 1, \\ T(n) &= aT(n-1) + n, \quad \text{for } n > 0. \end{aligned}$$

Prove that $T(n) = \Theta(a^n)$.

You might need the fact that, for any $x \neq 1$,

$$\sum_{i=1}^{n} ix^i = \frac{nx^{n+2} - (n+1)x^{n+1} + x}{(1-x)^2}.$$

Answer: By iterating the recurrence, we get

$$\begin{aligned} T(n) &= aT(n-1) + n \\ &= a^2T(n-2) + a(n-1) + n \\ &= a^3T(n-3) + a^2(n-2) + a(n-1) + n \\ &\quad \cdots \\ &= a^n + \sum_{i=1}^{n} a^{n-i}i \end{aligned}$$

Hence, we have

$$\begin{aligned} T(n) &= a^n + \sum_{i=1}^{n} a^{n-i}i \\ &= a^n + a^n \sum_{i=1}^{n} a^{-i}i \\ &= a^n + a^n \frac{n(\frac{1}{a})^{n+2} - (n+1)(\frac{1}{a})^{n+1} + (\frac{1}{a})}{(1-a)^2} \\ &= \Theta(a^n). \end{aligned}$$

Student ID: _____

Problem 9: [10 pts]
Consider a function $T(n)$ defined on integers n that are powers of 2. Suppose

$$\begin{aligned} T(1) &= 1, \\ T(n) &= 5T(n/2) + n^2, \quad \text{for } n > 1. \end{aligned}$$

Iterate the recurrence or use a recursion tree to find a closed-form expression for $T(n)$. Then simplify the closed-form expression using the big Θ notation.

Answer: [pts]

Let $n = 2^i$. Iterating the recurrence, we get

$$\begin{aligned} T(n) &= T(2^i) \\ &= 5T(2^{i-1}) + 2^{2i} \\ &= 5[5T(2^{i-2}) + 2^{2(i-1)}] + 2^{2i} \\ &= 5^2 T(2^{i-2}) + \frac{5}{4}2^{2i} + 2^{2i} \\ &= 5^3 T(2^{i-3}) + (\frac{5}{4})^2 2^{2i} + \frac{5}{4}2^{2i} + 2^{2i} \\ &\vdots \\ &= 5^i T(2^{i-i}) + (\frac{5}{4})^{i-1} 2^{2i} + \ldots + \frac{5}{4}2^{2i} + 2^{2i} \\ &= 5^i + 2^{2i}\frac{(\frac{5}{4})^i - 1}{\frac{5}{4} - 1} \\ &= 5 \cdot 5^i - 4 \cdot 4^i \\ &= 5 \cdot n^{\log_2 5} - 4n^{\log_2 4} \\ &= \Theta(n^{\log_2 5}). \end{aligned}$$

Student ID: _____

Problem 10: [10 pts]
A computer system considers a string of digits to be a valid code word if and only if it contains an even number of 0's. For instance, 1203045 is valid, whereas 780900 is not. Let V_n be the number of valid code words of length n.

It is clear that $V_1 = 9$ because "1", "2", ..., "9" are valid code words of length 1, while "0" is an invalid code word of length 1.

For $n > 1$, find a recurrence for V_n by determining how it is related to V_{n-1}. Solve the recurrence to get a closed-form formula for V_n.

Answer: A valid length n code can be obtained

- From a valid length $n-1$ code by appending "1", "2", ..., or "9"to the end, or
- From an invalid length $n-1$ code by appending "0" to the end.

The total number of length $n-1$ codes is 10^{n-1}. Hence the number of invalid length $n-1$ codes is $(10^{n-1} - V_{n-1})$. So, we have

$$V_n = 9V_{n-1} + (10^{n-1} - V_{n-1}) = 8V_{n-1} + 10^{n-1}.$$

Iterating the recurrence, we get

$$\begin{aligned}
V_n &= 8V_{n-1} + 10^{n-1} \\
&= 8(8V_{n-2} + 10^{n-2}) + 10^{n-1} \\
&= 8^2 V_{n-2} + 8 \times 10^{n-2} + 10^{n-1} \\
&= \ldots \\
&= 8^{n-1}V_1 + 8^{n-2} \times 10 \ldots + 8 \times 10^{n-2} + 10^{n-1} \\
&= 9 \times 8^{n-1} + 8^{n-2} \times 10 \times (1 + \frac{10}{8} + \ldots + (\frac{10}{8})^{n-2} + (\frac{10}{8})^{n-2}) \\
&= 9 \times 8^{n-1} + 8^{n-2} \times 10 \times \frac{(\frac{10}{8})^{n-1} - 1}{\frac{10}{8} - 1}) \\
&= 9 \times 8^{n-1} + \frac{10^n - 10 \times 8^{n-1}}{2} \\
&= \frac{1}{2}10^n + \frac{1}{2}8^n.
\end{aligned}$$

Student ID: _____

Scrap Paper 1

Student ID: _____

Scrap Paper 2

Student ID: _____

Scrap Paper 3